Herramientas de comunicación segura en Colombia: análisis técnico-legal

Resumen

Esta investigación documenta y analiza las herramientas de comunicación segura disponibles para ciudadanos colombianos, evaluando sus características técnicas frente al marco legal vigente. Mediante un diseño documental, se identifica una tensión fundamental: las herramientas que maximizan la privacidad técnica (como Signal) son arquitectónicamente incompatibles con las obligaciones de entrega de información establecidas en el Artículo 44 de la Ley 1621 de 2013, mientras que herramientas de adopción masiva (como WhatsApp) almacenan metadatos extensos que permiten el cumplimiento legal. El análisis examina cinco herramientas (PGP, Signal, WhatsApp, Tor, HTTPS/DoH), documentando cómo incluso las arquitecturas más seguras pueden ser circunvaladas si el usuario no configura correctamente los backups en servicios de terceros (ConsumerRights.wiki, s.f.-a), y cómo el uso de herramientas de alta privacidad puede generar visibilidad adversa ante autoridades. La investigación explora tres casos colombianos de aplicación práctica del marco legal (SIC vs WhatsApp 2021, vulnerabilidades MiVacuna 2021, Sentencia T-453/2024), revelando una asimetría entre derechos formales y capacidad real de ejercerlos.

Palabras clave: comunicación segura; ciberseguridad; encriptación; privacidad digital; marco legal Colombia

Contacto

privacidadylibreexpresion@cocaine.ninja

Autores

Jackeline A. Castaño

Juan C. Ortiz

Medellín, Colombia

Publicación Original 16 Noviembre 2025

Marco Teórico

Esta investigación se fundamenta en la intersección entre las capacidades técnicas de herramientas de comunicación segura y el marco normativo colombiano que regula su uso. Los conceptos técnicos centrales incluyen la encriptación de extremo a extremo (E2E), que es un método de cifrado donde únicamente el emisor y el receptor poseen las claves necesarias para descifrar el contenido del mensaje. Esto significa que incluso si alguien intercepta la comunicación en tránsito, solo verá datos incomprensibles. Sin embargo, el E2E protege el contenido del mensaje, pero no los metadatos asociados a la comunicación.

Los metadatos son información sobre la comunicación: quién contactó a quién, en qué momento, por cuánto tiempo, desde qué ubicación, y usando qué dispositivo. Aunque no revelan el contenido del mensaje, estos datos son necesarios para el enrutamiento de las comunicaciones y frecuentemente constituyen el objetivo primario de la vigilancia legal. Los casos históricos de vigilancia documentados por las autoridades judiciales colombianas demuestran que los metadatos pueden ser tan reveladores como el contenido mismo, pues permiten construir perfiles detallados de contactos, movimientos y patrones de comportamiento (Consejo de Estado, 2022; Corte Suprema de Justicia, 2022).

El marco jurídico colombiano establece el derecho fundamental a la intimidad en el Artículo 15 de la Constitución Política de Colombia (1991), donde se consagra que las comunicaciones privadas son inviolables y solo pueden interceptarse mediante orden judicial fundamentada. La Ley 1581 de 2012 regula la protección de datos personales, estableciendo el principio de libertad que requiere consentimiento previo, expreso e informado del titular para el tratamiento de sus datos. No obstante, el Artículo 10 de esta ley establece excepciones en casos de seguridad nacional o cuando la información sea requerida por orden judicial.

Por su parte, la Ley 1621 de 2013 otorga facultades específicas a los organismos de inteligencia y contrainteligencia. El Artículo 44 de la Ley 1621 de 2013 obliga a los operadores de telecomunicaciones a suministrar "el historial de comunicaciones, datos técnicos de identificación, localización de celdas", pero introduce una cláusula crítica: "cuando sea técnicamente viable". Esta cláusula reconoce implícitamente que existen arquitecturas de comunicación que hacen físicamente imposible cumplir

con la solicitud. El Artículo 33 de la Ley 1621 de 2013 establece una reserva de treinta años sobre la información recopilada en actividades de inteligencia, aunque la Sentencia T-374/2020 de la Corte Constitucional aclaró que esta reserva no es oponible a autoridades judiciales.

La tensión central identificada en esta investigación es de naturaleza estructural: las herramientas que ofrecen mayor protección técnica implementan arquitecturas diseñadas para no almacenar información, haciendo técnicamente imposible cumplir con la solicitud de "historial de comunicaciones" del Artículo 44 de la Ley 1621 de 2013, porque dicho historial simplemente no existe en sus servidores. En contraste, las herramientas que sí almacenan metadatos extensos pueden cumplir técnicamente con las obligaciones legales, pero ofrecen menor protección de privacidad al usuario.

Metodología

Esta investigación emplea un enfoque cualitativo con alcance descriptivo-analítico y diseño documental. El objetivo general es documentar y analizar las herramientas de comunicación segura disponibles para ciudadanos colombianos, evaluando sus características técnicas, su conformidad con el marco legal vigente, y las implicaciones prácticas para los usuarios que adoptan herramientas de alta privacidad.

Los objetivos específicos abordan tres dimensiones complementarias. La dimensión técnica identifica y caracteriza las principales herramientas de comunicación segura accesibles desde Colombia (PGP, Signal, WhatsApp, Tor, HTTPS/DoH), evaluando sus ideas en encriptación, arquitectura de seguridad y manejo de metadatos. La dimensión legal expone y analiza el marco legal colombiano aplicable a la privacidad en comunicaciones digitales, identificando procesos de garantía, responsabilidades de las partes involucradas (Estado, empresas, usuarios) y consecuencias de incumplimiento mediante casos documentados de aplicación práctica.

La pregunta de investigación que orienta este estudio es: ¿Qué herramientas de comunicación segura están disponibles para ciudadanos colombianos y cuáles son sus limitaciones técnicas y legales? El análisis se basa en fuentes documentales escritas: textos legales consultados en bases oficiales (Función Pública), jurisprudencia obtenida de la Relatoría de la Corte Constitucional, documentación

técnica oficial de las herramientas analizadas (whitepapers, políticas de privacidad, transparency reports), y literatura académica especializada en seguridad de comunicaciones.

Se reconocen limitaciones metodológicas inherentes al diseño documental, como la dependencia de auditorías de seguridad publicadas sin realizar pruebas técnicas propias, y la imposibilidad de acceder a información sobre solicitudes de vigilancia amparada por la reserva legal de treinta años establecida en el Artículo 33 de la Ley 1621 de 2013. Los casos específicos colombianos incluidos (vulnerabilidades en la aplicación MiVacuna, orden de la Superintendencia de Industria y Comercio a WhatsApp) provienen de reportes técnicos y periodísticos especializados, y se presentan como indicios ilustrativos de la aplicación práctica del marco legal, reconociendo esta limitación metodológica explícitamente.

Estado de la Investigación

Revisión de Literatura Académica

La producción académica sobre la intersección entre herramientas de comunicación segura y el marco legal colombiano es limitada. Jiménez-Almeira y López (2023) documentan la evolución normativa en ciberseguridad desde la Ley 1273 de 2009 hasta políticas actuales de protección de infraestructura crítica. Prieto Cruz y Álvarez (2024) hallaron una madurez operativa de apenas 38% en una entidad pública colombiana, evidenciando brechas entre marco normativo e implementación práctica.

La literatura técnica internacional documenta vulnerabilidades estructurales de protocolos tradicionales. Rao (2023) confirma que el sistema SS7 carece de autenticación robusta, permitiendo localización fraudulenta de suscriptores. Peeters et al. (2018) demuestran que ataques de redirección de llamadas vía SS7 pueden detectarse midiendo latencia de audio.

Aplicación Práctica del Marco Legal en Colombia

La Superintendencia de Industria y Comercio (SIC) supervisa la Ley 1581 de 2012. En 2021, la SIC ordenó a WhatsApp ajustar su política de datos para usuarios colombianos, exigiendo conformidad con la regulación nacional y registro de bases de datos, ilustrando la responsabilidad de empresas extranjeras y la facultad supervisora del Estado.

La aplicación gubernamental MiVacuna (2021) reveló deficiencias en "privacidad por diseño": generaba códigos QR con URLs públicamente accesibles mostrando datos sensibles sin autenticación. Este incidente documenta la necesidad de fortalecer capacidades técnicas institucionales más allá del marco normativo.

La Sentencia T-453/2024 de la Corte Constitucional estableció obligaciones de transparencia para plataformas digitales en gestión de contenidos. El caso involucró bloqueo de cuenta TikTok sin notificación ni apelación clara. La Corte determinó que plataformas deben proporcionar mecanismos de defensa conforme a debido proceso, aunque ejercer estos derechos requiere acción judicial (tutela), inaccesible para la mayoría por complejidad y costo, evidenciando asimetría entre derechos formales y capacidad práctica.

Análisis de Herramientas de Comunicación Segura

PGP (Pretty Good Privacy) es un programa de cifrado que convierte mensajes en códigos incomprensibles excepto para el destinatario autorizado. Su problema crítico es la complejidad técnica: requiere generar claves digitales, intercambiarlas de forma segura y verificar identidades mediante cadenas de confianza. Esta complejidad impide la adopción masiva: prácticamente nadie en el público general usa PGP cotidianamente. Ofrece máxima protección criptográfica con mínima viabilidad práctica.

Signal es una aplicación de mensajería que cifra mensajes de extremo a extremo y está diseñada para no guardar información sobre conversaciones en sus servidores. Mientras WhatsApp almacena metadatos sobre quién habla con quién, cuándo y por cuánto tiempo, Signal solo guarda la fecha de creación de cuenta y última conexión. Todo lo demás no existe en servidores de Signal, haciendo técnicamente imposible cumplir con solicitudes del Artículo 44 de la Ley 1621 de 2013 porque el "historial de comunicaciones" solicitado no existe. Signal Foundation (2024) demuestra esto: ante orden judicial, solo entregaron fecha de creación y último acceso.

Signal presenta una limitación crítica: aunque no almacena mensajes, permite crear backups en servicios de nube como iCloud o Google Drive. Si el usuario no activa manualmente "backup encriptado", estos backups se almacenan sin protección de cifrado de extremo a extremo de Signal (ConsumerRights.wiki, s.f.-a). Apple (2023) y Google (2023) entregan datos ante órdenes legales válidas, representando una circunvalación de la arquitectura de Signal mediante configuración incorrecta del usuario.

WhatsApp implementa cifrado de extremo a extremo en contenido usando Signal Protocol, pero pertenece a Meta y almacena metadatos extensos. Según su política oficial (WhatsApp LLC, 2024) y documentación técnica (ConsumerRights.wiki, s.f.-b), almacena: número de teléfono, fecha de registro, lista de contactos sincronizada, información de grupos, última conexión, duración de sesiones, dirección IP y modelo de dispositivo. Estos metadatos permiten reconstruir la red social del usuario y sus patrones de comunicación, cumpliendo técnicamente con el Artículo 44 de la Ley 1621 de 2013, aunque el contenido permanece cifrado. Su adopción masiva global reduce la visibilidad adversa prácticamente a cero: usar WhatsApp es estadísticamente "normal", convirtiéndolo en la opción pragmática para usuarios que buscan protección de contenido sin destacar ante autoridades.

Tor (The Onion Router) es una red de anonimato que oculta la dirección IP real enrutando el tráfico a través de múltiples nodos encriptados, dificultando rastrear quién accede a qué sitios. Sin embargo, genera visibilidad adversa muy alta: los nodos de Tor son públicamente conocidos, por lo que aunque protege contenido y destino, el patrón de uso es fácilmente identificable para autoridades con capacidad de monitoreo de red. Tor proporciona anonimato de capa de red pero no cifra el contenido por sí solo, requiriendo combinación con herramientas como Signal para protección completa.

HTTPS y DNS sobre HTTPS (DoH) son estándares de seguridad web moderna. HTTPS cifra la conexión entre navegador y servidor web, protegiendo de interceptores en tránsito. DoH cifra consultas de nombres de dominio, ocultando al proveedor de internet qué sitios consulta el usuario. Al ser estándares universales, no generan fricción social ni visibilidad adversa. Su limitación crítica es que solo protegen el tránsito: el servidor destino y la empresa operadora aún pueden ver contenido en claro y almacenar registros de acceso, permitiendo cumplimiento del Artículo 44 de la Ley 1621 de 2013.

Conclusiones y Perspectivas del Estudio

La investigación identifica una dualidad irresoluble entre capacidad técnica y obligación legal: las herramientas que maximizan la privacidad mediante arquitecturas de no-almacenamiento (Signal) son estructuralmente incompatibles con las obligaciones de entrega de información del Artículo 44 de la Ley 1621 de 2013. Las herramientas que sí pueden cumplir técnicamente con solicitudes legales (WhatsApp) lo hacen a costa de almacenar metadatos extensos que permiten reconstruir redes sociales y patrones de comportamiento. No existe solución técnica que satisfaga simultáneamente la maximización de privacidad individual, el cumplimiento legal completo y la normalidad social.

El marco legal colombiano presenta una contradicción constitutiva entre la Ley 1581 de 2012 (que otorga al ciudadano el derecho a conocer el uso de sus datos) y la Ley 1621 de 2013 (que establece reserva de treinta años sobre información de inteligencia), creando una asimetría de poder donde el ciudadano común no puede auditar si fue objeto de vigilancia estatal ni ejercer efectivamente sus derechos de habeas data en contextos de inteligencia.

Críticamente, la seguridad prometida por Signal depende de que el usuario configure manualmente los backups encriptados. De lo contrario, la información que "no existe en servidores de Signal" sí existe en servidores de Apple o Google, accesible mediante órdenes legales válidas. Esto refuerza que la privacidad efectiva

no es un producto que se compra o descarga, sino un proceso que requiere responsabilidad compartida: empresas que diseñen sistemas con privacidad por defecto (incluyendo backups), un Estado con marco legal coherente y transparente, y usuarios informados sobre las configuraciones técnicas críticas de las que depende su seguridad real.

Para el usuario colombiano promedio preocupado por seguridad, WhatsApp representa el equilibrio pragmático: ofrece protección contra amenazas no estatales (delincuencia común, hackers) mediante cifrado de extremo a extremo del contenido, mientras que su adopción masiva reduce la visibilidad adversa. Sin embargo, este "compromiso razonable" implica aceptar que Estado y corporaciones tendrán acceso a metadatos de comunicaciones, que pueden ser tan reveladores como el contenido mismo.

Como perspectiva para investigación futura, se sugiere la necesidad de estudios empíricos sobre el comportamiento real de usuarios colombianos frente a estas herramientas, evaluando qué factores determinan la adopción de medidas de privacidad y si existe comprensión de las implicaciones técnicas y legales. Un análisis comparativo con marcos legales de otros países latinoamericanos podría identificar mejores prácticas regulatorias que equilibren las necesidades legítimas de seguridad nacional con la protección efectiva de derechos ciudadanos, y evaluar si existen modelos que resuelvan la tensión identificada entre arquitecturas de privacidad y obligaciones de cooperación con autoridades.

Referencias

ConsumerRights.wiki. (s.f.-a). *Signal cloud backups*. https://consumerrights.wiki/w/Signal_cloud_backups

ConsumerRights.wiki. (s.f.-b). *WhatsApp*. https://consumerrights.wiki/w/WhatsApp

Consejo de Estado de Colombia. (2022). *Sentencia 25001-23-26-000-2012-00198-01 (66603)*.

Corte Constitucional de Colombia. (1991). *Constitución Política de Colombia*. Gaceta Constitucional No. 114.

Corte Constitucional de Colombia. (2020). Sentencia T-374/20. https://www.corteconstitucional.gov.co/relatoria/2020/t-374-20.htm

Corte Constitucional de Colombia. (2024). Sentencia T-453/24. https://www.corteconstitucional.gov.co/relatoria/2024/T-453-24.htm

Corte Suprema de Justicia de Colombia, Sala de Casación Penal. (2022). *Sentencia SP3806-2022*.

Google LLC. (2023). *Transparency report: Requests for user information*. https://transparencyreport.google.com/user-data/overview

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y seguridad integral: Un análisis reflexivo sobre el avance normativo en Colombia. *Dialnet*. https://dialnet.unirioja.es/servlet/articulo?codigo=10050181

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial* No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Ley 1621 de 2013. Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia. *Diario Oficial* No. 48.764. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=52706

Peeters, C., Pulls, T., & Rashid, S. (2018). Sonar: Detecting SS7 redirection attacks with audio-based distance bounding. En *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 107-113). IEEE. https://doi.org/10.1109/SPW.2018.00023

Prieto Cruz, Y. A., & Álvarez Múnera, J. W. (2024). *La seguridad y privacidad de la información en una entidad pública del Estado colombiano*. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/60771/yaprietocr.pdf

Rao, V. S. (2023). *Analyzing communications and software systems security* [Tesis doctoral, Aalto University]. Aalto University Repository. https://aaltodoc.aalto.fi/server/api/core/bitstreams/e1724061-b5d7-4f28-a4d6-d23d5e86523a/content

Signal Foundation. (2024). *Government requests: Grand jury subpoena for Signal user data, Central District of California*. https://signal.org/bigbrother/cd-california-grand-jury/